IN THE UNITED STATES DISTRICT COURT
FOR MIDDLE DISTRICT OF ALABAMA

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH [redacted] THAT IS STORED AT PREMISES CONTROLLED BY GOOGLE

Case No. 13-mj-3026-DGW

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Tyson Imming, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with Immigration & Customs Enforcement, Homeland Security Investigations (hereinafter referred to as HSI), and have been so employed since April 17, 2006. Prior to April 17, 2006, I was employed as an Immigration Agent with ICE since March 1, 2003. Prior to March 1, 2003, I was employed with the Immigration and Naturalization Service as an Immigration Agent, Detention Enforcement Officer and a Border Patrol Agent. My duties as a Special Agent include the investigation of any criminal or administrative violations of the Immigration and Nationality Act and criminal violations involving the unlawful movement of people and goods within and out of the United States. As part of my regular duties, I investigate criminal violations relating to prostitution, particularly of aliens, the use of computers relating to aliens and prostitution, in violation of 18 U.S.C. § 1952(a)(3).

2. I have received training in the area of prostitution and have been involved in several investigations of these offenses as well as the unlawful harboring and transportation of females engaged in prostitution. I also have received training specific to the use of computers. I also have participated in the execution of numerous search warrants and enforcement actions, some of which involved harboring aliens, and/or the transportation of females engaged in prostitution offenses.

3. I make this affidavit in support of an application under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) for a search warrant for information associated with a certain email account – [redacted] – that is stored at premises owned, maintained, controlled, or operated by Google, an e-mail provider headquartered at 1600 Amphitheatre Parkway, Mountain View, CA 94043. The information to be searched is described in the following paragraphs and in **Attachment A**. The search warrant sought in this application would require Google to disclose to the government records and other information in its possession, pertaining to the subscriber or customer operating the web sites, including the contents of communications.

4. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

STATUTORY AUTHORITY

5. Section 1952(a)(3) makes it a federal crime to use any facility in interstate or foreign commerce with the intent to otherwise promote, manage, establish, carry on, or facilitate the promotion, management, establishment, or carrying on, of any unlawful activity and thereafter promotes, manages, establishes, carries on an unlawful activity or attempts to do so. This section defines an "unlawful activity" to include "prostitution offenses in violation of the laws of the State in which they are committed." 18 U.S.C. § 1952(a)(3) & (b). Illinois law prohibits prostitution. 720 Ill. Comp. Stat. § 5/11-14.

6. Title 18, United States Code, Section 2703(a) provides that, pursuant to a search warrant issued by a court of competent jurisdiction, a governmental entity may require a provider of electronic communication service to disclose the contents of an electronic communication that has been stored electronically for 180 days or less.

7. Title 18, United States Code, Section 2703(b)(1)(A) provides that, pursuant to a search warrant issued by a court of competent jurisdiction, a governmental entity may require a provider of remote computing service to disclose the contents of an electronic communication that has been stored electronically for more than 180 days.

8. Title 18, United States Code, Section 2703(c)(1)(A) provides that, pursuant to a search warrant issued by a court of competent jurisdiction, a governmental entity may require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications).

9. Title 18, United States Code, Section 2711 defines "remote computing service" as "the provision to the public of computer storage or processing services by means of an electronic communications system."

10. Title 18, United States Code, Section 2711 defines "governmental entity" to include any department or agency of the United States and defines "court of competent jurisdiction" to include any district court of the United States (including a magistrate judge of such a court) that has jurisdiction over the offense being investigated.

TECHNICAL BACKGROUND

11. In my training and experience, as well as, from information I have obtained through consultation with personnel trained in the investigation, seizure, and analysis of computers, electronic data, and electronic media, I have learned that Google provides a variety of on-line services, including electronic mail ("e-mail") access, to the general public. Subscribers obtain an account by registering with Google. During the registration process, Google asks subscribers to provide basic personal information.

Therefore, the computers of Google are likely to contain stored electronic communications (including retrieved and unretrieved e-mail for Google subscribers) and information concerning subscribers and their use of Google services, such as account access information, e-mail transaction information, and account application information.

12. In general, an e-mail that is sent to a Google subscriber is stored in the subscriber's "mail box" on Google servers until the subscriber deletes the e-mail. If the subscriber does not delete the message, the message can remain on Google servers indefinitely.

13. When the subscriber sends an e-mail, it is initiated at the user's computer, transferred via the Internet to Google's servers, and then transmitted to its end destination. Google often saves a copy of the e-mail sent. Unless the sender of the e-mail specifically deletes the e-mail from the Google server, the e-mail can remain on the system indefinitely.

14. A Google subscriber can also store files, including e-mails, address books, contact or buddy lists, pictures, and other files, on servers maintained and/or owned by Google.

15. Subscribers to Google might not store on their home computers copies of the e-mails stored in their Google account. This is particularly true when they access their Google account through the web, or if they do not wish to maintain particular e-mails or files in their residence.

16. In general, e-mail providers like Google ask each of their subscribers to provide certain personal identifying information when registering for an e-mail account. This information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative e-mail addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number).

17. E-mail providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via Google's website), and other log files that reflect usage of the account. In addition, e-mail providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the e-mail account.

18. In some cases, e-mail account users will communicate directly with an e-mail service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. E-mail providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications.

PROBABLE CAUSE

1. On January 24, 2013, I received information from Officer Greg Hosp of the Fairview Heights, IL Police Department (FHPD) concerning [redacted] believed to be engaged in [redacted] located at [redacted] Fairview Heights, IL, (hereinafter collectively referred to as the [redacted]).

2. FHPD Officer Hosp informed me that his agency has conducted surveillance, patrol activity, and local record checks related to the [redacted]. These efforts resulted in identifying information and encounters with the subjects [redacted] individuals, identified below, operate or work at the [redacted]:

[redacted]

3. The officers with FHPD indicated that not once during their surveillance did they see [redacted] leave the [redacted] after opening the business in the morning until closing in the evening, nor did they see any other women enter the [redacted] to work. The [redacted] and from [redacted] were observed arriving together in one vehicle and leaving together at the end of the work day. [redacted] would arrive and depart the [redacted] at different times throughout the day.

4. FHPD Officer Hosp also informed me that his law enforcement agency encountered [redacted] during a traffic stop on January 19, 2013. During this stop, the [redacted] drove [redacted] with [redacted]. Additional surveillance by the FHPD indicated the [redacted], Illinois, [redacted]. Documentation for the apartment lists [redacted] as residents, but not [redacted].

5. FHPD Officer Hosp further informed me that his law enforcement agency encountered [redacted] at approximately 5:30 PM on January 24, 2013, [redacted] after leaving [redacted]. [redacted] and is in the area to visit his girlfriend who lives in the [redacted]

6. The FHPD provided me with information received during local record checks on the [redacted], including city business occupancy information and city inspection and emergency contact information on file. Specifically, the Fairview Heights building

permit for the business was applied for by [redacted]. During this application process, [redacted] provided [redacted], but stated that he lived in [redacted].

7. Records from the fire inspector in Fairview Heights, Illinois indicate that [redacted]. Upon finding [redacted], the fire inspector informed [redacted].

8. Emergency contact information on file for the [redacted] with the FHPD indicates the business is owned by [redacted]. Both the owner and manager listed the same home address, [redacted], Fairview Heights, Illinois. The [redacted] city business license application indicates the business owner's name is [redacted] and the manager is [redacted].

9. Based on this information, on January 25, 2013, I conducted immigration computer indices checks to determine the immigration status of the [redacted] who work and/or operate the [redacted]. Records indicate that each individual is [redacted] and [redacted]. The following alien file numbers were found:

[redacted]

10. That same day, I provided Officer Hosp with digital file photographs for [redacted] from immigration records to confirm their identities. Officer Hosp reviewed these photographs and affirmed these [redacted] are the ones he has observed and encountered during his surveillance of the [redacted].

11. Additionally, I searched the Illinois Department of Financial & Professional Regulation's (IDFPR) website to determine if any of the three individuals [redacted] are licensed in the [redacted], as required by 225 ILCS 57/ the [redacted]. I did not find any records indicating [redacted] are licensed [redacted], although Officer Hosp discovered a possible match for [redacted]. Because the website has limited search functions, the results are inconclusive.

12. Also, on or about January 24, 2013, FHPD Officer Hosp also provided me with information that the [redacted] advertises on Craigslist.com. I know that the search function on this website will produce matches from approximately the two previous weeks of historical postings using a key-word search. I conducted searches on Craigslist on that date for [redacted] and found that several postings had been made for the [redacted] as often as once per day during this two week time period. Each posting had the following language:

[redacted]

[redacted]

13. The advertisement includes a photo of an [redacted] and [redacted] for the business location. Open source Internet searches for the image of the woman resulted in 68 matches with several different image resolutions and sizes on a variety of websites. No actual identity of this woman is known, nor have any FHPD Officers observed this woman working at the [redacted]

14. I requested records from Craigslist.com for account information and posting history for the classified advertisements found for the [redacted]. I received a response from this company indicating that during the time period of October 20, 2012, through February 7, 2013, [redacted] were made on Craiglist by user name: [redacted] and email address [redacted] Sixty (60) of these posts were received by Craigslist.com from the [redacted] address [redacted].

15. I conducted research on this [redacted] and discovered it is [redacted]. On February 8, 2013, I requested user account identifying information from [redacted] for three of the occasions that this [redacted] Craigslist.com to post classified advertisements found for the AMNS.

16. On March 1, 2013, I received information from [redacted] that this [redacted] is uniquely assigned to the following [redacted]:

Name: [redacted]
Date Established: 9/18/2012
Status: Open
[redacted]

17. On or about February 22, 2013, Officer Hosp provided three police reports documenting statements from client's who had patronized the [redacted] and had purchased a [redacted] and [redacted] services or had been offered additional [redacted] services, but refused. The following are summaries of each report:

a. Client 1

On December 21, 2012, a customer of the [redacted]

b. Client 2

On February 1, 2013, a customer of the [redacted]

c. Client 3

On February 19, 2013, a customer of the [redacted]

[redacted]

18. In January and February 2013, I am aware that the FHPD also stopped [redacted] of the [redacted] for traffic violations while conducting surveillance. [redacted]

19. On February 13, 2013, HSI and the FHPD conducted an operation to monitor an [redacted] while [redacted]

20. The [redacted].

21. On February 8, 2013, I conducted Internet inquiries for the [redacted] and discovered approximately [redacted] related to the [redacted] on the website [redacted] -St. Louis/Chicago section [redacted] is one of several known websites with information related to the St. Louis, Missouri, geographic area which is maintained for the purpose of posting and sharing reviews, experiences, prices, advice and warnings for other persons who patronize [redacted] as well as allow for individuals to advertise [redacted] services to this clientele. These posts are made anonymously through the use of a "user name." The services offered or reviews made rely heavily on the use of code words and abbreviations.

22. I found the following posts related to the [redacted]:

[redacted]

[redacted]

19. Based on the common use of the abbreviation [redacted] on this website and posted glossaries of terms and abbreviations found on similar websites, such as [redacted] it is believed this is an abbreviation for [redacted].

20. On March 7, 2013, [redacted] (f).

21. [redacted] has been in custody continuously [redacted]. Following [redacted] arrest, Officer Hosp and Special Agent Ruth Saunders, HSI, interviewed [redacted] following the waiver of her Miranda rights. [redacted].

22. Pursuant to the [redacted], agents with HSI seized two cellular telephones from the [redacted] Both [redacted] were [redacted] I turned this [redacted]. All of the [redacted] featured [redacted]. The [redacted] also had [redacted] from the account [redacted].

23. The other phone had a pink case and [redacted] admitted during [redacted] interview after waiving her Miranda rights that [redacted].

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

24. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Google to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

25. Based upon all of the above, there is probable cause to believe that [redacted] has used the [redacted] email account to post advertisements promoting or facilitating the promotion of [redacted] in violation of 18 U.S.C. § 1952(a)(3).

26. Therefore, based on my training and experience, and the facts as set forth in this affidavit, there is probable cause to believe that on the computer systems in the control of Google there exists evidence of a crime and contraband or fruits of a crime. Accordingly, a search warrant is requested.

27. This Court has jurisdiction to issue the requested warrant because it is "a court with jurisdiction over the offense under investigation." 18 U.S.C. § 2703(a).

28. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

29. I certify that all of the information set forth above is true and correct to the best of my knowledge and belief.

REQUEST FOR SEALING

30. I further respectfully request that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application and search warrant. I believe that sealing these documents is necessary because they pertain to an ongoing investigation. Based upon my training and experience, I have learned that online criminals actively search for criminal affidavits and search warrants via the internet, and disseminate them to other online criminals as they deem appropriate, e.g., by posting them publicly online through various forums. Premature disclosure of the contents of this affidavit and related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness, as well as the safety of the officers who execute the warrant.

Respectfully submitted,

Tyson Imming
Special Agent, Homeland Security Investigations

State of Illinois)
) SS.
County of St. Clair)

Subscribed to and sworn before me this 11th day of March, 2013, at East St. Louis, Illinois.

DONALD G. WILKERSON
United States Magistrate Judge

ATTACHMENT A

Place to Be Searched

This warrant applies to information associated with the Google email account [redacted] that is stored at premises owned, maintained, controlled, or operated by Google, a company headquartered at 1600 Amphitheatre Parkway, Mountain View, CA 94043.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Google

To the extent that the information described in Attachment A is within the possession, custody, or control of Google, Google is required to disclose the following information to the government for the email account listed in Attachment A:

(a) The contents of all e-mails stored in the account, including copies of e-mails sent from the account.

(b) All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the types of service utilized, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number).

(c) All records or other information stored by an individual using the account, including address books, contact and buddy lists, pictures, videos, and other files.

(d) All records pertaining to communications between Google and any person regarding the account, including contacts with support services and records of actions taken.

(e) A list of all Google services to which the holder of the account has subscribed.

(f) A list of any and all associated accounts.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of the statutes listed on the warrant involving Christopher Gunn including:

(a) Records relating to interstate extortion, threatening communications, the [redacted]

(b) Records relating to who created, used, or communicated with the account listed in Attachment A.